Soft Computing Techniques Help Assign Weights to Different Factors in Vulnerability Analysis

Beverly Rivera[1,2], Irbis Gallegos[1], and Vladik Kreinovich[2]
[1]Regional Cyber and Energy Security Center RCES
[2]Computational Science Program
University of Texas at El Paso
500 W. University
El Paso, TX 79968, USA
barivera@miners.utep.edu, irbisg@utep.edu, vladik@utep.edu

***Abstract*—The main objective of vulnerability analysis is to select the alternative which is the least vulnerable. To make this selection, we must describe the vulnerability of each alternative by a single number – then we will select the alternative with the smallest value of this vulnerability index. Usually, there are many aspects of vulnerability: vulnerability of a certain asset to a storm, to a terrorist attack, to hackers' attack, etc. For each aspect, we can usually gauge the corresponding vulnerability, the difficulty is how to combine these partial vulnerabilities into a single weighted value. In our previous research, we proposed an empirical idea of selecting the weights proportionally to the number of times the corresponding aspect is mentioned in the corresponding standards and requirements. This idea was shown to lead to reasonable results. In this paper, we provide a possible theoretical explanation for this empirically successful idea.**

I. Formulation of the Problem

Need for vulnerability analysis. When it turns out that an important system is vulnerable – to a storm, to a terrorist attack, to hackers' attack, etc. – we need to protect it. Usually, there are many different ways to protect the same system. It is therefore desirable to select the protection scheme which guarantees the largest degree of protection within the given budget. The corresponding analysis of different vulnerability aspects is known as it vulnerability analysis; see, e.g., [2], [8], [11], [12], [13], [14].

Vulnerability analysis: reminder. Among several possible alternative schemes for protecting a system, we must select a one under which the system will be the least vulnerable. As we have mentioned, there are many different aspects of vulnerability. Usually, it is known how to gauge the vulnerability v_i of each aspect i. Thus, each alternative can be characterized by the corresponding vulnerability values $(v_1, \ldots, v_n)$. Some alternatives results in smaller vulnerability of one of the assets, other alternatives leave this asset more vulnerable but provide more protection to other assets.

To be able to compare different alternatives, we need to characterize each alternative by a single vulnerability index v – an index that would combine the values $v_1, \ldots, v_n$ corresponding to different aspects: $v = f(v_1, \ldots, v_n)$.

If one of the vulnerabilities v_i increases, then the overall vulnerability index v must also increase (or at least remain the same, but not decrease). Thus, the combination function $f(v_1, \ldots, v_n)$ must be increasing in each of its variables v_i.

Vulnerability analysis: important challenge. While there are well-developed methods for gauging each aspect of vulnerability, there is no well-established way of combining the resulting values $v_1, \ldots, v_n$ into a single criterion $v = f(v_1, \ldots, v_n)$.

Usually, vulnerabilities v_i are reasonably small; so terms which are quadratic (or of higher order) in v_i can be usually safely ignored. As a result, we can expand the (unknown) function $f(v_1, \ldots, v_n)$ in Taylor series in v_i and keep only linear terms in this expansion. As a result, we get a linear dependence

$$v = c_0 + \sum_{i=1}^n c_i \cdot v_i$$

for some coefficients c_i.

Comparison between different alternatives does not change if we subtract the same constant c_0 from all the combined values: $v < v'$ if and only if $v - c_0 < v' - c_0$. Thus, we can safely assume that $v_0 = 0$ and

$$v = \sum_{i=1}^n c_i \cdot v_i.$$

Similarly, comparison does not change if we re-scale all the values, e.g., divide them by the same constant

$$\sum_{i=1}^n c_i.$$

This is equivalent to considering a new (re-scaled) combined function

$$f(v_1, \ldots, v_n) = \frac{\sum\limits_{i=1}^n c_i \cdot v_i}{\sum\limits_{i=1}^n c_i \cdot v_i} = \sum_{i=1}^n w_i \cdot v_i,$$

where

$$w_i \stackrel{\text{def}}{=} \frac{c_i}{\sum\limits_{j=1}^n c_j}.$$

For these new weights, we have

$$\sum_{i=1}^n w_i = 1.$$

The fact the function must be increasing implies that $w_i \geq 0$.

The important challenge is how to compute the corresponding weights w_i.

Heuristic solution. In [4], [15], [17], we proposed an empirical idea of selecting the weights proportionally to the the frequency with which the corresponding aspect is mentioned in the corresponding standards and requirements. This idea was shown to lead to reasonable results.

Remaining problem and what we do in this paper. A big problem is that the above approach is purely heuristic, it does not have a solid theoretical explanation.

In this paper, we provide a possible theoretical explanation for this empirically successful idea.

II. Possible Theoretical Explanation

Main idea. We consider the situation in which the only information about the importance of different aspects is how frequently these aspects are mentioned in the corresponding documents. In this case, the only information that we can use to compute the weight w_i assigned to the i-th aspect is the frequency f_i with which this aspect is mentioned in the documents. In other words, we take $w_i = F(f_i)$, where $F(x)$ is an algorithm which is used to compute the weight based on the frequency.

Our goal is to formulate reasonable requirements on the function $F(x)$ and find all the functions $F(x)$ which satisfy this requirement.

First requirement: monotonicity. The more frequently the aspect is mentioned, the more important it is; thus, if $f_i > f_j$, we must have $w_i = F(f_i) > F(f_j) = w_j$. In mathematical terms, this means that the function $F(f)$ must be *increasing*.

Second requirement: the weights must add up to one. Another natural requirement is that for every combination of frequencies $f_1, \ldots, f_n$ for which

$$\sum_{i=1}^{n} f_i = 1,$$

the resulting weights must add up to 1:

$$\sum_{i=1}^{n} w_i = \sum_{i=1}^{n} F(f_i) = 1.$$

We are now ready to formulate our main result.

Proposition 1. *Let $F : [0,1] \to [0,1]$ be an increasing function for which $\sum\limits_{i=1}^{n} f_i = 1$ implies $\sum\limits_{i=1}^{n} F(f_i) = 1$. Then, $F(x) = x$.*

Comment. So, it is reasonable to use the frequencies as weights. This justifies the above empirically successful heuristic idea.

Proof.

1°. Let us first prove that $F(1) = 1$.

This follows from our main requirement when $n = 1$ and $f_1 = 1$. In this case, the requirement

$$\sum_{i=1}^{n} F(f_i) = 1$$

leads to $F(f_1) = F(1) = 1$.

2°. Let us prove that $F(0) = 0$.

Let us consider $n = 2$, $f_1 = 0$, and $f_2 = 1$. Then,

$$\sum_{i=1}^{n} f_i = 1$$

and therefore,

$$\sum_{i=1}^{n} F(f_i) = F(0) + F(1) = 1.$$

Since we already know that $F(1) = 1$, we thus conclude that $F(0) = 1 - F(1) = 1 - 1 = 0$.

3°. Let us prove that for every $m \geq 2$, we have

$$F\left(\frac{1}{m}\right) = \frac{1}{m}.$$

Let us consider $n = m$ and

$$f_1 = \ldots = f_n = \frac{1}{m}.$$

Then,

$$\sum_{i=1}^{n} f_i = 1$$

and therefore,

$$\sum_{i=1}^{n} F(f_i) = m \cdot F\left(\frac{1}{m}\right) = 1.$$

We thus conclude that

$$F\left(\frac{1}{m}\right) = \frac{1}{m}.$$

4°. Let us prove that for every $k \leq m$, we have

$$F\left(\frac{k}{m}\right) = \frac{k}{m}.$$

Let us consider $n = m - k + 1$,

$$f_1 = \frac{k}{m}$$

and

$$f_2 = \ldots = f_{m-k+1} = \frac{1}{m}.$$

Then,

$$\sum_{i=1}^{n} f_i = 1$$

and therefore,

$$\sum_{i=1}^{n} F(f_i) = F\left(\frac{k}{m}\right) + (m-k)\cdot F\left(\frac{1}{m}\right) = 1.$$

We already know that

$$F\left(\frac{1}{m}\right) = \frac{1}{m}.$$

Thus, we have

$$F\left(\frac{k}{m}\right) = 1 - (m-k)\cdot F\left(\frac{1}{m}\right) =$$

$$1 - (m-k)\cdot\frac{1}{m} = \frac{k}{m}.$$

The statement is proven.

5°. We have already proven that for every rational number r, we have $F(r) = r$. To complete the proof, we need to show that $F(x) = x$ for every real number from the interval $[0,1]$, not only for rational numbers.

Let x be any real number from the interval $(0,1)$. Let

$$x = 0.x_1x_2\ldots x_n\ldots,\quad x_i \in \{0,1\},$$

be its binary expansion. Then, for every n, we have

$$\ell_n \stackrel{\text{def}}{=} 0.x_1\ldots x_n \le x \le u_n \stackrel{\text{def}}{=} \ell_n + 2^{-n}.$$

As n tends to infinity, we have $\ell_n \to x$ and $u_n \to x$.

Due to monotonicity, we have $F(\ell_n) \le F(x) \le F(u_n)$. Both bounds ℓ_n and u_n are rational numbers, so we have $F(\ell_n) = \ell_n$ and $F(u_n) \le u_n$. Thus, the above inequality takes the form $\ell_n \le F(x) \le u_n$. In the limit $n\to\infty$, when $\ell_n \to x$ and $u_n \to x$, we get $x \le F(x) \le x$ and thus, $F(x) = x$. The proposition is proven.

Possible fuzzy extension. Our current analysis is aimed at situations when we are absolutely sure which aspects are mentioned in each statement. In practice, however, standards and documents are written in natural language, and a natural language is often imprecise ("fuzzy"). As a result, in many case, we can only decide with some degree of certainty whether a given phrase refers to this particular aspect.

A natural way to describe such degrees of certainty is by using *fuzzy logic*, technique specifically designed to capture imprecision of natural language; see, e.g., [6], [10], [19]. In this case, instead of the exact frequency f_i – which is defined as a ratio

$$\frac{n_i}{N}$$

between the number n_i of mentions of the i-th aspect and the total number N of all mentions – we can use the ratio

$$\frac{\mu_i}{N},$$

where μ_i is a fuzzy cardinality of the (fuzzy) set of all mentions of the i-th aspects – which is usually defined as the sum of membership degrees (= degrees of certainty) for all the words from the documents.

III. Towards a More General Approach

What we did: reminder. In the previous section, we proved that if we select the i-th weight w_i depending only only on the i-th frequency, then the only reasonable selection is $F(x) = x$.

A more general approach. Alternatively, we can compute a "pre-weight" $F(f_i)$ based on the frequency, and then we can *normalize* the pre-weights to make sure that they add up to one, i.e., take

$$w_i = \frac{F(f_i)}{\sum\limits_{k=1}^{n} F(f_k)}.$$

Remaining problem. In this more general approach, how to select the function $F(f)$?

What we do in this section. In this section, we describe reasonable requirements on this function $F(f)$, and we describe all possible functions $F(f)$ which satisfy these requirements.

First requirement: monotonicity. Our first requirement is that aspects which are mentioned more frequently should be given larger weights. In other words, if $f_i > f_j$, then we should have

$$w_i = w_i = \frac{F(f_i)}{\sum\limits_{k=1}^{n} F(f_k)} > \frac{F(f_j)}{\sum\limits_{k=1}^{n} F(f_k)} = w_j.$$

Multiplying both sides of this inequality by the sum

$$\sum_{k=1}^{n} F(f_k),$$

we conclude that $F(f_i) > F(f_j)$, i.e., that the function $F(f)$ should be monotonic.

Second requirement: independence from irrelevant factors. Let us assume that we have four aspect, and that the i-th aspect is mentioned n_i times in the corresponding document. In this case, the frequency f_i of the i-th aspect is equal to

$$f_i = \frac{n_i}{n_1+n_2+n_3+n_4}.$$

Based on these frequencies, we compute the weights w_i, and then select the alternative for which the overall vulnerability

$$w_1\cdot v_1 + w_2\cdot v_2 + w_3\cdot v_3 + w_4\cdot v_4$$

is the smallest possible.

In particular, we may consider the case when for this particular problem, the fourth aspect is irrelevant, i.e., for which $v_4 = 0$. In this case, the overall vulnerability is equal to

$$w_1\cdot v_1 + w_2\cdot v_2 + w_3\cdot v_3.$$

On the other hand, since the fourth aspect is irrelevant for our problem, it makes sense to ignore mentions of this aspect, i.e., to consider only the values n_1, n_2, and n_3. In this approach, we get new values of the frequencies:

$$f_i' = \frac{n_i}{n_1+n_2+n_3}.$$

Based on these new frequencies f_i', we can now compute the new weights w_i', and then select the alternative for which the overall vulnerability

$$w_1' \cdot v_1 + w_2' \cdot v_2 + w_3' \cdot v_3$$

is the smallest possible.

The resulting selection should be the same for both criteria. As we have mentioned, the optimizing problem does not change if we simply multiple the objective function by a constant. So, if $w_i' = \lambda \cdot w_i$ for some λ, these two objective functions lead to the exact same selection. In this case, the trade-off

$$\frac{w_i}{w_j}$$

between each two aspects is the same:

$$\frac{w_i'}{w_j'} = \frac{w_i}{w_j}.$$

However, if we have a different trade-off between individual criteria, then we may end up with different selections. Thus, to make sure that the selections are the same, we must guarantee that

$$\frac{w_i'}{w_j'} = \frac{w_i}{w_j}.$$

Substituting the formulas for the weights into the expression for the weight ratio, we can conclude that

$$\frac{w_i}{w_j} = \frac{F(f_i)}{F(f_j)}.$$

Thus, the above requirement takes the form

$$\frac{F(f_i')}{F(f_j')} = \frac{F(f_i)}{F(f_j)}.$$

One can check that the new frequencies f_i' can be obtained from the previous ones by multiplying by the same constant:

$$f_i' = \frac{n_i}{n_1 + n_2 + n_3} =$$

$$\frac{n_1 + n_2 + n_3 + n_4}{n_1 + n_2 + n_3} \cdot \frac{n_i}{n_1 + n_2 + n_3 + n_4} =$$

$$k \cdot f_i,$$

where we denoted

$$k \stackrel{\text{def}}{=} \frac{n_1 + n_2 + n_3 + n_4}{n_1 + n_2 + n_3}.$$

Thus, the above requirement takes the form

$$\frac{F(k \cdot f_i)}{F(k \cdot f_j)} = \frac{F(f_i)}{F(f_j)}.$$

This should be true for all possible values of f_i, f_j, and k. Once we postulate that, we arrive at the following result.

Proposition 2. *An increasing function $F : [0,1] \to [0,1]$ satisfies the property*

$$\frac{F(k \cdot f_i)}{F(k \cdot f_j)} = \frac{F(f_i)}{F(f_j)}$$

for all possible real values k, f_i, and f_j if and only if $F(f) = C \cdot f^\alpha$ for some $\alpha > 0$.

Comments.

- The previous case corresponds to $\alpha = 1$, so this is indeed a generalization of the formula described in the previous section.
- If we multiply all the values $F(f_i)$ by a constant C, then the normalizing sum is also multiplied by the same constant, so the resulting weights do not change:

$$w_i = \frac{F(f_i)}{\sum_{k=1}^{n} F(f_k)} = \frac{C \cdot f_i^\alpha}{\sum_{k=1}^{n} C \cdot f_k^\alpha} = \frac{f_i^\alpha}{\sum_{k=1}^{n} f_k^\alpha}.$$

  Thus, from the viewpoint of application to vulnerability, it is sufficient to consider only functions

$$F(f) = f^\alpha.$$

Proof.

1°. First, it is easy to check that for all possible values C and $\alpha > 0$, the function $F(f) = C \cdot f^\alpha$ is increasing and satisfies the desired property. So, to complete our proof, we need to check that each increasing function which satisfies this property has this form.

2°. The desired property can be equivalently reformulated as

$$\frac{F(k \cdot f_i)}{F(f_i)} = \frac{F(k \cdot f_j)}{F(f_j)}.$$

This equality holds for all possible values of f_i and f_j. This means that the ratio

$$\frac{F(k \cdot f)}{F(f)}$$

does not depend on f, it only depends on k. Let us denote this ratio by $c(k)$. Then, we get

$$\frac{F(k \cdot f)}{F(f)} = c(k),$$

i.e., equivalently,

$$F(k \cdot f) = c(k) \cdot F(f).$$

3°. Since $k \cdot f = f \cdot k$, we have $F(k \cdot f) = F(f \cdot k)$, i.e.,

$$c(k) \cdot F(f) = c(f) \cdot F(k).$$

Dividing both sides by $c(k) \cdot c(f)$, we conclude that

$$\frac{F(f)}{c(f)} = \frac{F(k)}{c(k)}.$$

This equality holds for all possible values of f and k. This means that the ratio

$$\frac{F(f)}{c(f)}$$

does not depend on f at all, it is a constant. We will denote this constant by C. From the condition

$$\frac{F(f)}{c(f)} = C,$$

we conclude that $F(f) = C \cdot c(f)$. So, to prove our results, it is sufficient to find the function $c(f)$.

4°. Substituting the expression $F(f) = C \cdot c(f)$ into the formula $F(k\cdot f) = c(k)\cdot F(f)$, we get $C\cdot c(k\cdot f) = c(k)\cdot C\cdot c(f)$. Dividing both sides of this equality by C, we conclude that

$$c(k \cdot f) = c(k) \cdot c(f).$$

Let us use this equality to find the function $c(f)$.

5°. For $k = f = 1$, we get $c(1) = c(1)^2$. Since $c(k) \neq 0$, we conclude that $c(1) = 1$.

6°. Let us denote $c(2)$ by q. Let us prove that for every integer n, we have $c(2^{1/n}) = q^{1/n}$.

Indeed, for $f = 2^{1/n}$, we have

$$f \cdot f \cdot \ldots \cdot f \ (n \text{ times}) = 2,$$

thus,

$$q = c(2) = c(f) \cdot \ldots \cdot c(f) \ (n \text{ times}) = (c(f))^n.$$

Therefore, we conclude that indeed, $c(f) = 2^{1/n}$.

7°. Let us prove that for every two integers m and n, we have

$$c(2^{m/n}) = q^{m/n}.$$

Indeed, we have

$$2^{m/n} = 2^{1/n} \cdot \ldots \cdot 2^{1/n} \ (m \text{ times}).$$

Therefore, we have

$$c(2^{m/n}) = c(2^{1/n}) \cdot \ldots \cdot c(2^{1/n}) \ (m \text{ times}) = (c(2^{1/n})^m.$$

We already know that $c(2^{1/n}) = q^{1/n}$; thus, we conclude that

$$c(2^{m/n}) = (q^{1/n})^m = q^{m/n}.$$

The statement is proven.

8°. So, for rational values r, we have $c(2^r) = q^r$. Let us denote $\alpha \stackrel{\text{def}}{=} \log_2(q)$. By definition of a logarithm, this means that $q = 2^\alpha$. Thus, for $x = 2^r$, we have

$$q^r = (2^\alpha)^r = 2^{\alpha\cdot r} = (2^r)^\alpha = x^\alpha.$$

So, for values x for which $\log_2(x)$ is a rational number, we get $c(x) = x^\alpha$.

Similarly to the proof of Proposition 1, we can use monotonicity to conclude that this equality $c(x) = x^\alpha$ holds for all real values x. We have already proven that $F(x) = C \cdot c(x)$, thus we have $F(x) = C \cdot x^\alpha$. The proposition is proven.

IV. Possible Probabilistic Interpretation of the Above Formulas

Formulation of the problem. In the above text, we justified the empirical formula $F(x) = x$ without using any probabilities – since we do not know any probabilities that we could use here.

However, in the ideal situation, when we know the exact probability of every possible outcome and we know the exact consequences of each outcomes, a rational decision maker should use probabilities – namely, a rational decision maker should select an alternative for which the expected value of the utility is the largest; see, e.g., [3], [7], [9], [16].

From this viewpoint, it would be nice to show that the above heuristic solution is not only reasonable in the above abstract sense, but that it actually makes perfect sense under certain reasonable assumptions about probability distributions.

What we do in this section. In this section, on the example of two aspects v_1 and v_2, we show that there are probability distributions for which the weights w_i should be exactly equal to frequencies.

Towards a formal description of the problem. Let us assume that the actual weights of two aspects are w_1 and $w_2 = 1 - w_1$. Let us also assume that vulnerabilities v_i are independent random variables. For simplicity, we can assume that these two variables are identically distributed.

In each situation, if the first vulnerability aspect is more important, i.e., if $w_1\cdot v_1 > w_2\cdot v_2$, then the document mentions the first aspect. If the second vulnerability aspect is more important, i.e., if $w_1\cdot v_1 < w_2\cdot v_2$, then the document mentions the second aspect. In this case, the frequency f_i with which the first aspect is mentioned is equal to the probability that the first aspect is most important, i.e., the probability that $w_1 \cdot v_1 > w_2 \cdot v_2$:

$$f_1 = P(w_1 \cdot v_1 > w_2 \cdot v_2).$$

We would like to justify the situation in which $f_i = w_i$, so we have

$$w_1 = P(w_1 \cdot v_1 > w_2 \cdot v_2).$$

This equality must hold for all possible values of w_1.

Analysis of the problem and the resulting solution. The desired equality can be equivalently reformulated as

$$P\left(\frac{v_1}{v_2} > \frac{w_2}{w_1}\right) = w_1.$$

Since $w_2 = 1 - w_1$, we get

$$P\left(\frac{v_1}{v_2} > \frac{1 - w_1}{w_1}\right) = w_1.$$

To simply computations, it is convenient to use logarithms: then ratio become a difference, and we get

$$P(\ln(v_1) - \ln(v_2) > z) = w_1,$$

where we denoted

$$z \stackrel{\text{def}}{=} \ln\left(\frac{1 - w_1}{w_1}\right).$$

Let us describe w_1 in terms of z. From the definition of z, we conclude that

$$e^z = \frac{1 - w_1}{w_1} = \frac{1}{w_1} - 1.$$

Thus,

$$\frac{1}{w_1} = 1 + e^z,$$

and

$$w_1 = \frac{1}{1 + e^z}.$$

So, we conclude that

$$P(\ln(v_1) - \ln(v_2) > z) = \frac{1}{1 + e^z}.$$

The probability of the opposite event $\ln(v_1) - \ln(v_2) \le z$ is equal to one minus this probability:

$$P(\ln(v_1) - \ln(v_2) \le z) = 1 - \frac{1}{1 + e^z} = \frac{e^z}{1 + e^z}.$$

This means that for the auxiliary random variable

$$\xi \stackrel{\text{def}}{=} \ln(v_1) - \ln(v_2),$$

the cumulative distribution function $F_\xi(z) \stackrel{\text{def}}{=} P(\xi \le z)$ is equal to

$$F_\xi(z) = \frac{e^z}{1 + e^z}.$$

This distribution is known as a *logistic* distribution; see, e.g., [1], [5], [18].

It is known that one way to obtain a logistic distribution is to consider the distribution of $\ln(v_1) - \ln(v_2)$, where v_1 and v_2 are are independent and exponentially distributed. Thus, the desired formula $w_i = f_i$ (i.e., $F(x) = x$) corresponds to a reasonable situation when both vulnerabilities are exponentially distributed.

ACKNOWLEDGMENTS

This work was supported by the University of Texas at El Paso Regional Cyber and Energy Security Center (RCES) supported by the City of El Paso's Planning and Economic Development division.

This work was also supported in part by the National Science Foundation grants HRD-0734825 and HRD-1242122 (Cyber-ShARE Center of Excellence) and DUE-0926721.

REFERENCES

[1] N. Balakrishnan, *Handbook of the Logistic Distribution*. Marcel Dekker, New York, 1992.

[2] Department of Energy, *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*, Version 1.0, 2012, available at http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model-es-c2m2

[3] P. C. Fishburn, *Nonlinear Preference and Utility Theory*, John Hopkins Press, Baltimore, Maryland, 1988.

[4] I. Gallegos et al., *System, Method and Apparatus for Assessing a Risk of one or More Assets within an Operational Technology Infrastructure*, US Patent No. 61/725,474, 2012.

[5] N. L. Johnson, S. Kotz, and N. Balakrishnan, *Continuous Univariate Distributions*, Vol. 2, Wiley, New York, 1995.

[6] G. Klir and B. Yuan, *Fuzzy Sets and Fuzzy Logic*, Prentice Hall, Upper Saddle River, New Jersey, 1995.

[7] R. D. Luce and R. Raiffa, *Games and Decisions: Introduction and Critical Survey*, Dover, New York, 1989.

[8] National Electric Sector CyberSecurity Organization Resource (NESCOR), *Electric Sector Failure Scenarios and Impact Analyses*, Version 1.0, 2012, available at http://www.smartgrid.epri.com/nescor.aspx

[9] H. T. Nguyen, V. Kreinovich, B. Wu, and G. Xiang, *Computing Statistics under Interval and Fuzzy Uncertainty*, Springer Verlag, Berlin, Heidelberg, 2012.

[10] H. T. Nguyen and E. A. Walker, *A First Course in Fuzzy Logic*, Chapman and Hall/CRC, Boca Raton, Florida, 2006.

[11] National Institute of Standard and Technology (NIST), *Guide for Mapping Types of Information and Information Systems for Security Categories*, NIST Special Publication 800-60, Volume 1, Revision 1, 2008.

[12] National Institute of Standard and Technology (NIST), *Guide for Conducting Risk Assessment*, NIST Special Publication 800-30, Revision 1, 2011.

[13] National Institute of Standard and Technology (NIST), *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82, 2011.

[14] National Institute of Standard and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Revision 4, 2012.

[15] L. Perez, *Regional Cyber and Energy Security (RCES) Center 2012 Annual Progress Report – Year 1*, El Paso, Texas, June 2013, available as https://www.elpasotexas.gov/muni_clerk/agenda/07-30-13/07301315C.pdf

[16] H. Raiffa, *Decision Analysis*, McGraw-Hill, Columbus, Ohio, 1997.

[17] Regional Cyber and Energy Security (RCES) Center at the University of Texas at El Paso, *Developing a Framework to Improve Critical Infrastructure Cyber Security*, National Institute for Standards and Technology (NIST) Report, April 2013, available as http://csrc.nist.gov/cyberframework/rfi_comments/rces_center_040113.pdf

[18] D. J. Sheskin, *Handbook of Parametric and Nonparametric Statistical Procedures*, Chapman & Hall/CRC, Boca Raton, Florida, 2011.

[19] L. A. Zadeh, "Fuzzy sets", *Information and Control*, 1965, Vol. 8, pp. 338–353.